General Assembly

Raised Bill No. 5816

February Session, 2008

LCO No. **2747**

*02747_____ET_*

Referred to Committee on Energy and Technology

Introduced by:
(ET)

AN ACT CONCERNING INTERNET SECURITY.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective from passage*) As used in sections 1 to 3, inclusive, of this act:

(1) "Availability" means the timely and reliable access to and use of information created, generated, collected or maintained by a state agency;

(2) "Communications and information resources" means (A) procedures, equipment and software designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information; and (B) associated personnel, including consultants and contractors;

(3) "Confidentiality" means the preservation of authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information;

(4) "Searchable web site" means a web site that allows the public to search or aggregate information;

(5) "Information security" means the protection of communication and information resources from unauthorized access, use, disclosure, disruption, modification or destruction to (A) prevent improper information modification or destruction; (B) preserve authorized restrictions on information access and disclosure; (C) ensure timely and reliable access to and use of information; and (D) maintain the confidentiality, integrity and availability of information;

(6) "Information security plan" means the plan developed by a state agency pursuant to sections 1 to 3, inclusive, of this act;

(7) "Institution of higher education" means a state-supported institution of higher education;

(8) "Integrity" means the prevention of improper information modification or destruction and ensuring information nonrepudiation and authenticity;

(9) "Expenditure of state funds" (A) means the expenditure of all appropriated or nonappropriated funds by a state entity from the Treasury in forms including, but not limited to, grants, contracts, subcontracts, tax refunds, rebates or credits, excluding those which result from the overpayment of income tax, or expenditures pursuant to any compact between the Governor and a federally recognized Indian tribe or nation in this state. (B) "Expenditure of state funds" shall not mean the transfer of funds between two state agencies or payments of state or federal assistance to an individual; and

(10) "Security incident" means an accidental or deliberative event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption or destruction of communication and information resources.

Sec. 2. (NEW) (*Effective from passage*) The Governor shall appoint a chief information security officer with experience in security and risk management for communications and information resources. Said

chief information security officer's duties shall include, but not be limited to, (1) developing and updating information security procedures, standards and guidelines for all state agencies; (2) ensuring the incorporation of and compliance with information security policies, standards and guidelines in the information security plans developed by state agencies pursuant to sections 1 to 3, inclusive, of this act; (3) directing information security audits and assessments in state agencies to ensure program compliance; (4) establishing and directing a risk management process to identify information security risks in state agencies and deploy risk mitigation strategies, processes and procedures; (5) reviewing and approving state agency information security plans annually; and (6) conducting information security awareness training programs.

Sec. 3. (NEW) (*Effective from passage*) (a) On or before the start of each fiscal year, each state agency shall develop an information security plan using the information security policies, standards and guidelines developed by the chief information security officer appointed pursuant to section 2 of this act. Said plans shall provide information security for the communication and information resources that support the operations and assets of each state agency.

(b) Information security plans developed pursuant to subsection (a) of this section shall include, but not be limited to (1) periodic assessments of the risk and magnitude of the harm that could result from a security incident; (2) a process for providing adequate information security for the communication and information resources of the state agency; (3) periodic security awareness training to inform the agency's employees and users of the agency's communication and information resources about information security risks and the responsibility of employees and users to comply with agency policies, standards and procedures designed to reduce those risks; (4) periodic vulnerability assessment testing and evaluation of the effectiveness of information security for the state agency, which shall be performed not less than annually; (5) a process for detecting, reporting and

responding to security incidents consistent with the information security standards, policies and guidelines issued by the chief information security officer; and (6) plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of the state agency during a security incident.

(c) On or before the beginning of each new fiscal year, each state agency shall submit the information security plan developed pursuant to subsection (a) of this section to the chief information security officer for approval.

(d) If a state agency fails to submit an information security plan to the chief information security officer on or before the beginning of the new fiscal year or if the chief information security officer disapproves said plan, the officer shall notify the Governor and the agency head of the agency in question. If no plan has been approved by October first of any year, the officer may suspend the operation of said agency's communication and information resources until such plan has been submitted to and approved by the officer.

(e) Information security plans developed pursuant to this section may provide for a phase-in period not to exceed three years. Any plan providing for such a phase-in period shall include an implementation schedule for such period.

(f) On or before the beginning of each new fiscal year, the head of each state agency shall report to the chief information security officer on the development, implementation and, if applicable, compliance with the phase-in schedule of the state agency's security plan. On or before January 1, 2010, and annually thereafter, the chief information security officer shall report, in accordance with section 11-4a of the general statutes, to the Governor and the joint standing committee of the General Assembly having cognizance of matters relating to technology concerning the implementation of the provisions of plans developed pursuant to this section.

Sec. 4. (NEW) (*Effective from passage*) (a) No later than January 1, 2009, the Office of Policy and Management shall develop and operate a single, searchable web site accessible by the public at no cost to access which shall include:

(1) For each expenditure:

(A) The name of the principal location or residence of the recipient of the funds;

(B) The amount of the state funds expended;

(C) The type of transaction;

(D) The funding or expending agency;

(E) The budgetary source of the funds;

(F) A description of the purpose of the expenditure; and

(G) Any other relevant information specified by the state Finance Office.

(2) The complete contents of the tax expenditure report published by the Department of Revenue Services.

(b) The web site established pursuant to section 4 of this act shall include data for the fiscal year beginning January 1, 2008, and each fiscal year thereafter. Such data shall be available on such web site no later than thirty days after the last day of the preceding fiscal year.

(c) The Department of Revenue Services, the Treasurer and any other state agency shall provide to the Office of Policy and Management the information necessary to accomplish the purposes of this section.

(d) Nothing in this section shall be interpreted to require the disclosure of information considered confidential by state or federal

law.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*from passage*	New section
Sec. 2	*from passage*	New section
Sec. 3	*from passage*	New section
Sec. 4	*from passage*	New section

Statement of Purpose:

To develop information security standards, policies and guidelines at all state agencies and to appoint a chief information security officer to manage the state's information security initiatives.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]